

## 🚀 Plan de Estudio – Hacking Ético (Red Team)

Este plan es **paralelo a tu carrera de Desarrollo de Software**, para que aprendas hacking mientras fortaleces tu base en programación.

📅 **Duración estimada:** 6-12 meses (según tu ritmo, con 1-2 horas diarias).

🚀 **Objetivo:** Dominar técnicas de pentesting, exploit development y ataques ofensivos.

---

### 💠 1. Fundamentos Esenciales (1-2 meses)

#### ✅ Sistemas Operativos:

- Profundizar en **Linux** (Kali Linux, Debian)
- Manejo de terminal y scripting en **Bash**

#### ✅ Redes y Seguridad:

- Modelos OSI y TCP/IP
- Protocolos (HTTP, TCP, UDP, ARP, DNS, ICMP)
- Firewalls, NAT, VPN y proxies

#### ✅ Python para Hacking:

- Uso de **Scapy** (manipulación de paquetes)
- Automatización de ataques con **pwntools**

#### ✅ Herramientas Básicas de Pentesting:

- **Nmap** (escaneo de redes)
  - **Wireshark** (análisis de tráfico)
  - **Metasploit** (exploits automatizados)
- 

### 💠 2. Hacking Web y Explotación de Vulnerabilidades (2-3 meses)

#### ✅ OWASP Top 10:

- **SQL Injection** → Cómo inyectar y prevenirlo
- **XSS (Cross-Site Scripting)** → Robo de cookies y ataques en navegadores
- **CSRF, SSRF, RCE, LFI, RFI** → Vulnerabilidades en aplicaciones web

✓ **Herramientas clave:**

- **Burp Suite** → Análisis y manipulación de tráfico
- **SQLmap** → Automatización de SQL Injection
- **Gobuster, Dirb** → Fuerza bruta en directorios

✓ **Hacking en APIs y aplicaciones móviles**

---

◆ **3. Pentesting de Infraestructura y Redes (2-3 meses)**

✓ **Ataques en redes locales (LAN):**

- **MITM (Man-in-the-Middle)** → Ataques con ARP Spoofing
- **Sniffing** → Captura de tráfico con Wireshark
- **Desautenticación WiFi** (Ataques a redes WPA/WPA2)

✓ **Pentesting en Active Directory**

- Enumeración y explotación de redes Windows
- Uso de **BloodHound, CrackMapExec, Responder**

✓ **Explotación de vulnerabilidades en servidores**

- Escalada de privilegios en Linux/Windows
  - Automatización con **LinPEAS y WinPEAS**
- 

◆ **4. Desarrollo de Exploits y Evasión de Seguridad (3 meses o más)**

✓ **Exploit Development con Python y C**

- Creación de **Buffer Overflows**
- Análisis de memoria con **GDB, Immunity Debugger**

✓ **Bypassing Antivirus y EDR**

- Ofuscación de payloads en **Metasploit**
- **Veil, Shellter** para evitar detección

✓ **Ataques avanzados (Red Team)**

- **Cobalt Strike, Empire, Havoc** → Frameworks de post-explotación

- **Phishing y ataques de ingeniería social**
- 

### **Cómo estudiar este plan**

✦ **Herramientas clave:** Aprende a usarlas en laboratorios virtuales (**TryHackMe**, **Hack The Box**, **VulnHub**).

✦ **Ejercicios prácticos:** Participá en **CTFs (Capture The Flag)** como Hack The Box Academy.

✦ **Certificaciones recomendadas:**

- **eJPT** (para empezar)
- **OSCP** (nivel avanzado)

## 🧠 FASE 1: Fundamentos Esenciales (1-2 meses)

### 📖 Libros / Teoría:

- 📖 “Linux Basics for Hackers” – OccupyTheWeb
- 📖 “The Linux Command Line” – William E. Shotts
- 📖 “How the Internet Really Works” – Article 19

### 💻 Cursos:

- 📺 TryHackMe – Complete Beginner Path (*¡Perfecto para comenzar!*)
- 📺 [Curso de Redes desde cero – YouTube \(Fernando Pérez\)](#)
- 📺 Linux para Hackers – Curso en Udemy

### 🔧 Herramientas a practicar:

- nmap, wireshark, netstat, iptables, bash, curl, dig
  - Python: scapy, socket, os, subprocess
  - Práctica con Kali Linux o Parrot OS
- 

## 🕸 FASE 2: Hacking Web y Vulnerabilidades OWASP (2-3 meses)

### 📖 Libros / Teoría:

- 📖 “Web Hacking 101” – Peter Yaworski
- 📖 “The Web Application Hacker’s Handbook” – Dafydd Stuttard (referencia total)
- 📖 OWASP Top 10 → <https://owasp.org/www-project-top-ten/>

### 💻 Cursos:

- 📺 TryHackMe – Web Fundamentals + OWASP
- 📺 PortSwigger Web Security Academy (*GRATIS, nivel profesional*)
- 📺 Curso “Hacking Ético Web” de Udemy (buscalo por ofertas)




### 🔧 Herramientas:

- Burp Suite
- SQLmap




- Gobuster / Dirb
  - Nikto / Wfuzz
  - Firefox + extensiones para testing web (HackBar, FoxyProxy)
- 

### **FASE 3: Pentesting de Infraestructura y Redes (2-3 meses)**

#### **Libros:**

-  “*The Hacker Playbook 3*” – Peter Kim
-  “*Red Team Field Manual (RTFM)*” – Michael Sikorski
-  “*Advanced Penetration Testing*” – Wil Allsopp

#### **Cursos:**




-  **TryHackMe – Offensive Pentesting Path**
-  **Hack The Box Academy – Network Pentesting**
-  **Practical Ethical Hacking – The Cyber Mentor (Udemy)**

#### **Herramientas:**

- Netcat, Hydra, Responder, CrackMapExec, BloodHound
  - LinPEAS / WinPEAS
  - Impacket (psexec, smbclient, secretsdump)
  - Ataques de fuerza bruta, escaneos SMB, enum4linux
- 

### **FASE 4: Desarrollo de Exploits y Red Teaming (3 meses o más)**

#### **Libros / Teoría:**

-  “*Black Hat Python*” – Justin Seitz
-  “*The Art of Exploitation*” – Jon Erickson
-  “*The Shellcoder's Handbook*” – Chris Anley

#### **Cursos:**

-  **Buffer Overflow Prep – TryHackMe**

- 📁 [Exploit Development – Offensive Security Exploit Developer (OSED)]
- 📁 Curso “Malware Development” – Zero2Automated (avanzado)

#### 🔧 Herramientas:

- GDB, Radare2, Immunity Debugger
- Metasploit, Veil, MSFvenom, Shellter
- Cobalt Strike / Havoc Framework
- Python (pwntools), Assembly (nasm/x86/x64)

#### 🚀 Extras muy recomendados

#### 📁 Plataformas para practicar:

- [TryHackMe](#) (*ideal para empezar*)
- [Hack The Box](#) (*más desafiante*)
- [Root Me](#)
- [VulnHub](#) (*máquinas vulnerables para VirtualBox/Kali*)

#### 🎓 Certificaciones por nivel:

Nivel	Certificación
● Básico	eJPT (INE)
● Intermedio	PNPT (TCM Security) / CEH
● Avanzado	OSCP (Offensive Security) / CRTO

🟢 **Nivel Básico: eJPT (eLearnSecurity Junior Penetration Tester)**

✅ **Dificultad: Baja a intermedia**

💰 **Precio: Aproximadamente \$200 USD**

📄 **Descripción:**

- Es una excelente certificación inicial para comenzar en el mundo de la **ciberseguridad ofensiva**.
- Cubre conocimientos básicos de **pentesting**, redes y vulnerabilidades.
- El examen es **práctico** y simula un entorno real de pruebas, lo que lo hace perfecto para principiantes.
- El contenido se basa en el curso **eLearnSecurity Penetration Testing** (también puedes acceder a él por separado si lo prefieres).

🏆 **Ideal para ti: Si estás comenzando en pentesting, es una certificación muy recomendada para hacer el puente entre la teoría y la práctica.**

---

🟡 **Nivel Intermedio: CEH (Certified Ethical Hacker)**

✅ **Dificultad: Media**

💰 **Precio: Aproximadamente \$1000 USD (a veces hay ofertas)**

📄 **Descripción:**

- Es una de las certificaciones más reconocidas y populares en el mundo de la **ciberseguridad**.
- Cubre un amplio rango de **herramientas y técnicas** para realizar pentests, enfocados en pruebas de **penetración** en redes, sistemas, aplicaciones web, etc.
- El curso está más enfocado en **conceptos y herramientas** que en práctica directa, aunque la certificación requiere de una buena preparación en la parte práctica.
- Puedes optar por **Tomar el curso oficial** o **prepararte por tu cuenta**, pero te exigen un conocimiento básico de redes y programación.

🏆 **Ideal para ti: Es una buena opción si ya tienes alguna base en pentesting, te dará una visión global y es muy útil para quienes desean entrar al mundo profesional.**

---

● **Nivel Avanzado: OSCP (Offensive Security Certified Professional)**

✅ **Dificultad: Alta**

💰 **Precio: Aproximadamente \$800 USD (por el curso + examen)**

📄 **Descripción:**

- Es una de las certificaciones más **prestigiosas y desafiantes** en el mundo de la ciberseguridad.
- Se enfoca completamente en **pentesting práctico**, en la cual deberás hackear sistemas, ganar acceso y escalar privilegios de manera realista.
- El examen es un desafío de **24 horas**, en el que deberás **hackear** varias máquinas dentro de un entorno controlado.
- **Requiere conocimientos previos** sólidos en redes, programación y herramientas de pentesting.

🏆 **Ideal para ti: Si deseas una certificación avanzada que te abra puertas en el mundo de la ciberseguridad profesional, y estás listo para enfrentar el desafío de aprender con la práctica.**

---

🧠 **Recomendación Final:**

**Si recién comenzás:**

- **eJPT** es la opción más accesible y adecuada, porque te permite adquirir experiencia práctica sin que el precio o la dificultad te agobien.

**Si tenés más experiencia en ciberseguridad y ya manejas conceptos básicos:**

- **CEH** es un excelente paso intermedio. Te dará una **visión más amplia** de las herramientas y técnicas utilizadas en la industria.

**Si te sentís listo para un reto grande:**

- **OSCP** es la certificación más desafiante y prestigiosa, pero te exigirá una sólida preparación en pentesting práctico y **al menos 6 meses de experiencia** previa.